# UNITED STATES DISTRICT COURT

for the

Central District of California

| | | |
|---|---|---|
| In the Matter of the Search of<br>*The person of JIAN XIN* | )<br>)<br>) | Case No. **2:24-MJ-01386** |

**APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

*See Attachment A-2*

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

*See Attachment B*

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| 18 U.S.C. § 501 | Use and Possession of Counterfeit Postage |
| 18 U.S.C. § 371 | Conspiracy to Defraud the United States |

The application is based on these facts:

*See attached Affidavit*

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (*give exact ending date if more than 30 days*: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*/s/ Tony Yu*

*Applicant's signature*

U.S. Postal Inspector Tony Yu

*Printed name and title*

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: _____

*Judge's signature*

City and state: Los Angeles, CA

U.S. Magistrate Judge Pedro V. Castillo

*Printed name and title*

AUSA: K. Afia Bondero (x2435)

**ATTACHMENT A-2**

PERSON TO BE SEARCHED

The person of JIAN XIN, who is described as an Asian male, approximately 5'05" tall, with black hair, black eyes, and California Driver's License number ending in -6663.

The search of the aforementioned person shall include any and all clothing and personal belongings, including any digital devices, backpacks, wallets, briefcases and bags that are within XIN's immediate vicinity and control at the location where the search warrant is executed. The search shall not include a strip search or a body cavity search.

**ATTACHMENT B**

**I. ITEMS TO BE SEIZED**

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 501 (Possession and Use of Counterfeit Postage) and 18 U.S.C. § 371 (Conspiracy to Defraud the United States) ("the SUBJECT OFFENSES"), namely:

a. Packages with altered, forged, counterfeited, or falsely made mailing labels;

b. Computers, cell phones, or any other mechanisms and items, including computer programs and applications, printers, and label materials that can be used to create or alter a USPS postage label or meter stamp or create counterfeit postage;

c. Altered, forged, counterfeited, or falsely made mailing labels;

d. Records, including correspondence and other communications, referring or relating to U.S. postage, including altered or counterfeit postage;

e. Receipts, or other payment records, relating to U.S. postage, including altered or counterfeit postage;

f. Records identifying the owners, shareholders, principals, employees, and ownership structure of any business operating at the SUBJECT PREMISES;

2. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the SUBJECT OFFENSES, and forensic copies thereof;

3. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted;

b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment of other devices;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. evidence of the times the device was used;

f. applications, programs, software, documentation, manuals, passwords, keys, and other access devices that may be necessary to access the device or data stored on the device, to run software contained on the device, or to conduct a forensic examination of the device;

g. records of or information about Internet Protocol addresses used by the device.

4. As used herein, the terms "records," "information," "documents," "programs," "applications," and "materials" include records, information, documents, programs, applications, and materials created, modified, or stored in any form, including in

digital form on any digital device and any forensic copies thereof.

5. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

## II. SEARCH PROCEDURE FOR DIGITAL DEVICES

6. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar

facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the scope of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase," "Griffeye," and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items

to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

d. If the search determines that a digital device does not contain any data falling within the scope of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the scope of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the scope of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling

outside the scope of the items to be seized absent further order of the Court.

7. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

8. During the execution of this search warrant, law enforcement is permitted to: (1) depress XIN's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of XIN's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

9. The special procedures relating to digital devices found in this warrant govern only the search of digital devices

pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

# AFFIDAVIT

I, Tony Yu, being duly sworn, declare and state as follows:

## I. INTRODUCTION

1. I am a Postal Inspector with the United States Postal Inspection Service ("USPIS"). I was employed as a Postal Inspector from September 2012 through August 2014 and again since September 2022. I am currently assigned to the Los Angeles Division of USPIS, specifically, to the Fraud Team Revenue Investigation, which is responsible for investigating fraud against the United States Postal Service ("USPS"). From September 2014 through August 2022, I was employed as a Special Agent by the USPS Office of Inspector General investigating USPS internal crimes. From June 2008 through May 2012, I was a California Peace Officer employed by California Medical Board investigating criminal and administrative violations perpetrated by physicians.

## II. PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of a search warrant for the following premises and person: Whizzotech Corporation ("Whizzotech") located at 1773 W. San Bernardino Rd. Suite E74 and Suite E75, West Covina, CA 91790 ("the SUBJECT PREMISES"), more fully described in Attachment A-1, and the person of Jian Xin ("XIN"), more fully described in Attachment A-2, for the items to be seized described in Attachment B, which are the evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 501 (Possession and Use of Counterfeit Postage) and 18

U.S.C. § 371 (Conspiracy to Defraud the United States) (the "Subject Offenses").

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only, all amounts or sums are approximate, and all dates and times are on or about those indicated.

## III. SUMMARY OF PROBABLE CAUSE

4. The USPIS is investigating Whizzotech Corp. and its owner Jian Xin ("XIN") for a counterfeit postage fraud scheme occurring within the Central District of California. XIN operates a business involved in the resell of consumer goods. Most of the postage used by XIN and his business to ship goods within the United States are counterfeit that appear to be obtained from an individual in China. XIN and his employees are believed to be responsible for the attempted introduction of thousands of parcels bearing counterfeit postage into the USPS mail stream, including at least approximately $289,777.33 in postage losses for 15,674 total shipments from September 28, 2023, to January 24, 2024.

5. The SUBJECT PREMISES is a warehouse used by XIN and his employees to process and ship mail parcels containing counterfeit postage. Xin purchases counterfeit postage from a Chinese individual, then prints the counterfeit postage for use at the SUBJECT PREMISES.

6. On March 8, 2024, the grand jury returned an indictment against XIN for violations of the SUBJECT OFFENSES. See 24-CR-157-MWF. Law enforcement intends to simultaneously execute this search warrant and the arrest warrant of XIN that was issued concurrent with the filing of the indictment.

## IV. STATEMENT OF PROBABLE CAUSE

### A. Background on USPS Postage

7. The USPS offers many postal services, including the delivery of parcels. All mailable articles shipped within the U.S. must comply with established mailing standards published in the USPS Domestic Mail Manual, including standards for weight, minimum/maximum dimensions, acceptable containers, proper sealing/closing, markings, and restrictions on items such as hazardous materials.

8. Moreover, all mail pieces must bear appropriate valid postage. The mailer is responsible for proper payment of postage and all mail must be fully prepaid at the time of the mailing. Postage payment is shown in the form of stamps, stamped stationary, precanceled stamps, postage meter imprints and PC postage[1] products or permit imprint (collectively,

[1] PC Postage (also known as "personal computer postage") refers to postage that is meant to be printed by the customer.

referred to as "indicia"), as well as via shipping label(s) purchased online and printed by the customer on standard paper (e.g., Click-N-Ship).

9. A postage evidencing system is a device or system of components a customer uses to print indicia such as Information-Based Indicia("IBI") or Intelligent Mail Indicia ("IMI") to indicate postage payment. Customers print indicia directly on a mail piece or on a label that is affixed to a mail piece.

10. The scheme at issue in this investigation involves the use of invalid PC Postage shipping labels. PC Postage shipping labels are comprised of various components, each providing substantive information to the USPS regarding the mail item being shipped. Some of the PC postage components provide information in a format that can be read by the human eye ("human-readable format"), while other components, such as IBI, contain data-matrix barcodes that can only be processed and deciphered by a computer ("machine-readable format"). The human-readable and machine-readable components of PC Postage items contain some of the same categories of information (e.g., weight, tracking number, date of purchase).

11. When attempting to determine whether an item of PC postage is counterfeit, USPIS and USPS personnel will frequently look to see if any of the unique identifiers on the postage are either invalid or inconsistent with other information on the shipping label.

**B. Investigation into XIN and WHIZZOTECH**

12. Based on my conversations with other law enforcement agents, I am aware of the following:

a. On or about June 1, 2021, a USPIS Revenue Fraud Analyst ("RFA") detected mail parcels shipped by Whizzotech Corp. bearing counterfeit USPS mail labels. The counterfeit postage items were designed to mimic postage pre-paid shipping labels purchased from internet-based postage providers. In addition, the return address used on most of the mail listed "Whizzotech Corp. 204 S 5th Ave. City of Industry, CA 91746" as the sender. The real property located at 204 S. 5th Avenue in the City of Industry, California is a commercial warehouse facility. A USPS official notification was sent to Whizzotech Corp. via mail and advised on the illegality of using counterfeit postage. An unidentified Whizzotech Corp. representative stated in an email that the counterfeit mail labels were provided to them by an unidentified Chinese national named "Peter."

b. On or about August 18, 2023, another USPIS RFA saw a driver for Whizzotech Corp., Xiaobin Chen ("CHEN"), dropping off a truckload of mail all bearing counterfeit postage at the Walnut Post Office in Walnut, California. Similar to the counterfeit postage discovered in June 2021, the counterfeit postage items were designed to mimic postage pre-paid shipping labels purchased from internet-based postage providers. CHEN signed a cease and desist form in Chinese on behalf of Whizzotech Corp. promising to stop using counterfeit postage.

13. On or about November 15, 2023, XIN opened PO Box 3029, Covina, California 91722 under his own name. USPIS determined that the PO Box was listed as the sender and return address on counterfeit postage labels used by Whizzotech Corp. According to California DMV records, XIN stands approximately 5'05" tall, has black hair, black eyes, and a California Driver's License number ending in -6663.

14. On or about December 5, 2023, I, along with other USPIS postal inspectors and RFAs, conducted a knock and talk[2] at at Whizzotech's then-business location at 204 S 5th Ave, City of Industry, CA 91746. During the visit, we observed in plain view that employees at the facility were printing USPS mail labels and labeling mail parcels for shipment. Two RFAs identified the mail labels as counterfeit. The counterfeit postage items were designed to mimic postage pre-paid shipping labels purchased from internet-based postage providers, as seen in the prior counterfeit postage originating from Whizzotech. In addition, the return address used on many of the mail labels listed "PO Box 3029 Covina, CA 91722," owned by XIN, as the return address and sender.

15. During a non-custodial interview[3] that I conducted with XIN, he admitted to the following information:

---

[2] During business hours, we went to Whizzotech Corp., identified ourselves as Postal Inspectors, and asked to speak to the owner.

[3] We explained the purpose of our visit to investigate the counterfeit mail labels, and XIN spoke to us as he walked us around the warehouse, showing us his operations, and we also spoke in his office.

a. He is the owner of Whizzotech Corp. and his company operates e-commerce stores as well as fulfillment orders for other e-commerce vendors.

b. He is aware of the USPIS notification of counterfeit postage usage from on or about June 1, 2021 as well as the signed Voluntary Discontinuance from on or about August 18, 2023 promising to stop using counterfeit postage.

c. XIN admitted he is the owner of PO Box 3029, Covina, California 91722.

d. He cannot afford to purchase postage directly from USPS due to the high cost. XIN instead purchases USPS postage from an unidentified company from China at an 8% discount rate from the USPS rate.

16. During the interview, XIN was asked to provide documentation to show payment for postage. XIN subsequently changed his story a few different times and was unable to produce any proof of payment for postage. XIN then voluntarily showed a WeChat[4] conversation with an unidentified individual with a screen picture of Jerry the mouse from the cartoon Tom and Jerry and Chinese name pronounced Chao SU ("SU"). The messages from this individual contained PDF files with embedded USPS postage labels. XIN opened one of the PDF files from his personal computer and an RFA verified the postage labels contained within were counterfeit.

[4] WeChat is a Chinese messaging application.

a. XIN stated SU is not his employee and he does not know his identity. XIN also stated SU is a Chinese national residing in China.

b. XIN stated his employees send shipping data from Whizzotech Corp. to SU daily. SU in return sends back a PDF file containing postage labels for all the parcels each day. The postage labels are then printed and used in the operations of Whizzotech Corp.

c. XIN consented to a voluntary search of his WeChat messages with Jerry. A separate chat history between XIN and SU was discovered. The chat history showed XIN giving SU instructions to change the sender information on the mailing labels to the sender name consistent with his PO Box 3029, as well as XIN sending electronic payment to SU in Chinese Yuan. XIN ended the consent search of his phone when questioned about the payment. XIN stated the payment was for work SU did for him and he refused to answer further questions about SU.

d. XIN was asked why he continues to use counterfeit postage labels when he has been notified on multiple occasions. XIN stated, "everyone uses it, it's not just me."

17. USPIS postal inspectors also observed outgoing mail bearing counterfeit postage labels in plain view organized into different mail sacks ready for shipment. XIN admitted this mail is destined to be dropped off at different Post Offices. XIN stated he uses Covina, El Monte and Walnut Post Offices to mail parcels. XIN stated he did not do this to avoid detection of counterfeit postage. XIN stated his belief that USPS requires

mail to be dropped off at post offices matching the sender's city. XIN agreed all the outgoing mail sent by Whizzotech Corp. originated from the warehouse in La Puente, regardless of the listed sender address on the mail label.

18. XIN signed another Voluntary Discontinuance form promising to stop using counterfeit postage labels.

19. Based on reviewing a completed PO Box application form, on or about December 12, 2023, PO Box 2939, Covina, California 91722 was opened under NianJun Xing ("XING"), who is XIN's spouse. California Secretary of State shows XING as an agent for Whizzotech Corp.

20. From on or about December 19, 2023, an RFA seized approximately nine pallets of mail parcels to date that were dropped off at Covina Post Office from Whizzotech Corp. bearing counterfeit postage. The counterfeit postage items were designed to mimic postage pre-paid shipping labels purchased from internet-based postage providers, as the others originating from Whizzotech. In addition, the return address used on many of the mail labels listed "PO Box 2939 Covina, CA 91722" as the return address and sender, which matches the PO Box that XING opened approximately one week after XIN's interview.

21. As of January 26, 2024, an RFA had identified seven Mailer Identification (MID)[5] account numbers hijacked by Whizzotech Corp. for use on their counterfeit postage. The RFA collected USPS mailing data using machine-run data from

[5] MID is a mailer identification number aka account number assigned to businesses that have registered an account.

September 28, 2023, to January 24, 2024. The data shows an estimated $289,777.33 in postage losses for 15,674 shipments in total that are attributed to these seven identified MID accounts.

22. On or about February 26, 2024, Whizzotech's location was changed on the California Secretary of State website to 1773 W. San Bernardino Rd., #E75, West Covina, California 91790.

23. Based on a conversation I had with a USPIS RFA, I am aware that on or about March 4, 2024, Covina Post Office intercepted two pallets of mail bearing counterfeit postage labels from Whizzotech.

24. Based on another conversation I had with a USPIS RFA, I am aware that on or about March 7, 2024, Montebello Post Office intercepted one pallet of mail bearing counterfeit postage labels from Whizzotech.

25. On or about March 8, 2024, I along with a USPIS RFA visited Whizzotech's prior location at 204 S. 5th Ave. in La Puente, California 91746. Whizzotech is no longer at this location, and the location now houses a vehicle parts business.

26. On or about March 8, 2024, I along with a USPIS RFA visited Whizzotech's new listed address located at 1773 W. San Bernardino Rd. #E75 in West Covina, California. Upon arriving at the location, the rollup gate to the unit was open and in plain view were outgoing mail parcels sorted into USPS mail bags. XIN was observed standing out front giving instructions to employees. The RFA and I approached XIN, and he agreed to speak with us. During that conversation, XIN stated the

following. XIN stated he has moved to this new location approximately one month ago, he now rents two units at this location, E74 and E75, which are joined units (i.e. the "SUBJECT PREMISES"). XIN stated he now purchases USPS mail labels from a new individual in China named "David." XIN stated the new individual also gives him an 8% discount on the face value of the labels as he can not afford to buy directly from USPS.

27. After we finished speaking with XIN, we noticed that the mail parcels we had initially seen through the rollup gate had been moved to an adjacent open air parking lot. There were also now parked vehicles in front of the mail, and the entrance gate was locked. I requested to inspect the mail locked behind the gate and XIN stated the area and mail belongs to another unidentified company and they (i.e., he and Whizzotech) don't have access to it. XIN later changed his story and had one of his employees open the gate. I observed approximately 500 pieces of outgoing parcels all with random shipping addresses. The RFA confirmed only a few pieces of this mail had legitimate postage while the rest bore counterfeit postage labels.

### C. XIN is Indicted for Conspiracy and Use/Possession of Counterfeit Postage

28. On March 8, 2024, a grand jury in the Central District of California returned an indictment against XIN for violations of 18 U.S.C. § 371 (Conspiracy to Defraud the United States) and 18 U.S.C. § 501 (Possession and Use of Counterfeit Postage) (i.e., the SUBJECT OFFENSES). See 24-CR-157-MWF. Law enforcement intends to simultaneously execute this search

warrant and the arrest warrant of XIN that was issued concurrent with the filing of the indictment.

## V. TRAINING AND EXPERIENCE ON THE SUBJECT OFFENSES

29. Based on my training and experience as well as conversation with other law enforcement officers and experts, I am aware that typical production and usage of counterfeit USPS postage labels operates as follows:

a. I understand many e-commerce vendors in the U.S. are engaged in the reselling of low cost, bulky and heavy consumer goods on various e-commerce platforms for profit. Due to the low cost and bulky, heavy nature of the items, in order to make a profit, vendors seek to reduce or eliminate the cost of shipping by knowingly purchasing and or creating counterfeit USPS postage labels.

b. Individuals involved in creating counterfeit USPS postage labels usually work with computer programmers often based in China to decipher the machine-readable format portion of the postage label. Counterfeit labels are then created with altered machine-readable format portion of the postage label to fool USPS machines into thinking payment has been made.

c. In making the counterfeit postage labels a source MID account needs to be associated and is accomplished by hijacking existing MID account numbers belonging to various entities. To continuously operate a business involved in shipping products, shipping information needs to be routinely provided to computer programmers who can then embed such information on to the counterfeit postage labels.

## VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

30. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the

form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

31. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so

many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

32. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after

a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress XIN's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of XIN's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

## VII. CONCLUSION

33. For all the reasons described above, there is probable cause to believe that the items listed in Attachment B, which constitute evidence, fruits, and instrumentalities of violations of the Subject Offenses will be found at the SUBJECT PREMISES and on the person of XIN as described in Attachment A-1 and A-2.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this ____ day of March, 2024.

_____

HONORABLE PEDRO V. CASTILLO
UNITED STATES MAGISTRATE JUDGE